



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/645,376	08/24/2000	Michael Scott Probasco	NC13977	3555

7590 04/08/2005

Nokia Inc  
6000 Connection Drive 1-4-755  
Irving, TX 75039

EXAMINER
----------

CALLAHAN, PAUL E

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 04/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/645,376	<b>Applicant(s)</b> PROBASCO, MICHAEL SCOTT	
	<b>Examiner</b> Paul Callahan	<b>Art Unit</b> 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 06 December 2004.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Amendment***

1. Claims 1-12 were pending in this application at the time of the previous Office Action. New claims 13-18 have been added by the latest amendment. Therefore claims 1-18 are pending and have been examined.

### ***Response to Arguments***

2. The applicant asserts that the claimed invention may be distinguished from the teaching of the Wasilewski '474 Patent because it does not teach combining the hashed key and encrypted data in a broadcast message that can be decrypted by each of a plurality of receiving nodes. Yet a careful reading of the Wasilewski Patent shows that the message sent by the broadcast center is capable of being utilized by any of a plurality of receiving nodes that are authorized according to an encapsulation protocol, the illustrative embodiment taught by Wasilewski is not fairly limited to a single receiving node but instead teaches a multicast system that reads on the claim language of claims 1, 6, 8, and 11.

The Applicant asserts that the Wasilewski '474 patent does not teach a hashed key that is also used to encrypt the data. Yet such is indeed taught at col. 3 lines 43-67, and col. 4 lines 1-25. As stated in col. 4 of the Wasilewski Patent: "...*a method and apparatus are provided for generating a message authentication code comprised of a hash of the first key and the second key, such that the STU can determine if the packets bearing the first key has been tampered with during transmission*".

In traverse of the rejection of claim 4, the Applicant asserts that no comparison is made between a prestored key and a hashed version included in a broadcast message. Yet a careful reading of Wasilewski shows that such is indeed taught at col. 11 lines 30-50.

In traverse of the rejection of claims 9 and 10, the applicant asserts that Wasilewski fails to teach sending a request for a key to a network entity if no matching key is found. Yet such is taught at col. 11 lines 48-50.

### ***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 15-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The phrase "...a broadcast message that is independent of any representation of a key..." is unclear as to what characteristic the message must have.

### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2137

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claims 1, 2, 4-6, and 8-12 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Wasilewski et al. US 5,870,474.

As for claims 1, 6, 8, and 11, Wasilewski teaches a method and means for carrying out the method for sending secure messages in a broadcast network (abstract) comprising the steps of: encrypting data with a key (col. 3 lines 43-67); hashing said key (col. 4 lines 1-25), combining said encrypted data and said key in a broadcast message capable of being decrypted by each of a plurality of receiving nodes (col. 3 lines 43-67), and transmitting said broadcast message to the plurality of receiving nodes (abstract).

As for claim 2, Wasilewski teaches a plurality of keys (col. 3 lines 43-67), and a combining step that comprises combining said encrypted data with each one of said plurality of different keys in a plurality of broadcast messages (abstract, col. 4 lines 1-25), and transmitting one of the plurality of broadcast messages to a subset of said plurality of receiving nodes (abstract).

As for claims 4, 9, and 10, Wasilewski teaches a method and means for carrying out the method for decrypting a message received over a broadcast network (abstract) comprising the steps of: receiving data comprising an encrypted message and a hashed key at a node in said broadcast network (abstract) where said node comprises means for storing data (fig. 1 items 90a – 90n “Customers STU’s”); parsing said data to derive said encrypted message and said hashed key (col. 11 lines 24-30); comparing said received hashed key with a plurality of keys pre-stored in said means for storing data in

Art Unit: 2137

said node and to select a key having a hash matching said received hashed key and decrypting said encrypted message with said matching key if a match is found (col. 11 lines 24-67).

As for claim 5, Wasilewski teaches requesting a key from a network entity if no prestored key has a hash that matches said received key (col. 11 lines 48-50).

As for claim 12, Wasilewski teaches a tangible medium that is a hard disk or the like (fig. 11 item 196).

As for claim 14, Wasilewski teaches parsing, comparing, and decrypting steps that are carried out at each of a plurality of nodes (col. 11 lines 24-67)

### ***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski as applied to claim 5 above, and Official Notice.

Wasilewski teaches all of the limitations of claim 5 upon which claim 7 is dependent but doesn't teach a network entity that distributes hashed keys as per claim 7. Official Notice may be taken however that such a feature is old and well known in the art of cryptographic communications. Therefore it would have been obvious to one of

Art Unit: 2137

ordinary skill in the art at the time of the invention to incorporate this feature into the system of Wasilewski. It would have been desirable to do so as to increase the security of key distribution. Wasilewski discusses the advantage of making this combination at for example col. 4 lines 1-25 where the desirability of transmitting keys in hashed form is explained.

### ***Conclusion***

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent document teaches a system of multicast pertinent to the applicant's disclosure:

Russ et al.            US 6,748,080

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

Art Unit: 2137

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (703) 305-1336. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

4/2/05



**ANDREW CALDWELL  
SUPERVISORY PATENT EXAMINER**